

LIST OF THE CLAIMS

1. (Currently Amended) A method for verifying port mapping integrity in a network, comprising:
 - accessing port binding information, which includes an identification and an authorized port of an authorized service, in a port authorization file in said network;
 - querying a port mapper for a mapped port assignment, which was created when an application registered a service provided by the application with said port mapper at the time said application was brought up, said mapped port assignment includes a current port used by said registered service;
 - determining if said identified service is currently using said authorized port by comparing said mapped port assignment to said port binding information; and
 - initiating a response to said comparing.
2. (Original) The method described in Claim 1 wherein said network comprises a utility data center.
3. (Original) The method described in Claim 1 wherein said mapped port assignment comprises static port binding data.
4. (Original) The method described in Claim 1 wherein said port authorization file comprises fixed port assignments.
5. (Original) The method described in Claim 1 wherein said port authorization file is generated upon network initialization.
6. (Original) The method described in Claim 1 wherein said response comprises an alarm.
7. (Original) The method described in Claim 1 wherein said response comprises a system lockdown.

8. (Currently Amended) In a network comprising a plurality of network port connections, a network port map verification tool, comprising:
- a port assignment file comprising a port authorization, which includes an authorized port of an authorized service, in said network; and
 - a port assignment file verifier wherein said verifier is enabled to verify a port assignment against said port authorization by,
 - querying a port mapper for a mapped port assignment, which was created when an application registered a service provided by the application with said port mapper at the time said application was brought up, said mapped port assignment includes a current port used by said registered service;
 - determining if said identified service is currently using said authorized port by comparing said mapped port assignment to said port binding information; and
 - initiating a response to said comparing.
9. (Original) The network port map verification tool described in Claim 8 , wherein said network comprises a utility data center.
10. (Original) The network port map verification tool described in Claim 9, wherein said network port map verification tool is further enabled to initiate a response to a port assignment anomaly.
11. (Original) The network port map verification tool described in Claim 10, wherein said response is an alarm.
12. (Original) The network port map verification tool described in Claim 10, wherein said response is a system lockdown.
13. (Original) The network port map verification tool described in Claim 9, wherein said network port map verification tool is enabled to verify a digital signature related to said port authorization.

14. (Original) The network port map verification tool described in Claim 9, wherein said network port map verification tool is enabled to operate in a remote procedure call environment.

15. (Currently Amended) A system for protecting network security, comprising:
a network server coupled to a network;
a network client communicatively coupled with said network server via a port;
a plurality of provisionable services enabled to communicate with said server via a plurality of ports; and
a port map verification tool enabled to compare a port assignment to a port authorization, which includes an authorized port of an authorized service, in said network by,
querying a port mapper for a mapped port assignment, which was created when an application registered a service provided by the application with said port mapper at the time said application was brought up, said mapped port assignment includes a current port used by said registered service;
determining if said identified service is currently using said authorized port by comparing said mapped port assignment to said port binding information; and
initiating a response to said comparing.

16. (Original) The system for protecting network security described in Claim 15 wherein said network comprises a utility data center.

17. (Original) The system for protecting network security described in Claim 15, wherein said port map verification tool is enabled to initiate a response to a port assignment anomaly.

18. (Original) The system for protecting network security described in Claim 17, wherein said response can be an alarm.

19. (Original) The system for protecting network security described in Claim 17, wherein said response can be a system lockdown.

20. (Original) The system for protecting network security described in Claim 17, wherein said port map verification tool is enabled to operate in a remote procedure call environment.